7. SYSTEM BACK-UPS AND RECOVERY

7.1 System Back-ups

System back-ups are an integral part of any automatic data processing (ADP) environment. Thus, the strongest defense against lost data is to keep good back-ups and to understand the procedures for restoring a file(s) or an entire file system. There are several types/kinds of back-ups that should be performed on a regular and fixed schedule that will minimize system downtime.

- Types of Back-up. In most ADP environments, there are two types of back-up; full and incremental. A full-system back-up will back-up all the file systems at the time it is executed. An incremental back-up records only those files that have changed within the listed time period, such as the last 24 hours.

- Full System Back-up. Full system back-up should be executed, periodically. For a full system back-up of all UNIX system files, perform the following tasks:

  - Login as root.

  - Open a terminal window.

  - Insert a 4mm Dat tape

  - Type ./Fullsys (upon completion, label tape "AFMIS Full System Backup" write date and block number(s) on label.

  - Close Terminal window.

- Incremental Back-ups. The incremental back-ups in the AFMIS environment are daily, weekly, and monthly.

- Daily Back-ups. Daily system back-ups should be accomplished by the SA to capture files that have changed within the past 24 hours. The daily back-up should be run at the same time(s) during the day to assure all data is captured. The SA can invoke the process directly from the command line. This can be done during the EOD process. However, you must ensure that no one is logged-on the system, and you are logged-in as "root".

In order to perform a daily back-up, the AFMIS SA must:

- Make sure no user is on the system.
- Login as root.
- Open a Terminal Window.
- Insert a tape into the tape drive.
- Type /osexec/sysbkp or cd /osexec; . / daily.

The following menu should be displayed:

MENU FOR BACKUP

D DAILY
W WEEKLY
M MONTHLY
X EXIT

OPTION:

Enter D for Daily.

SELECT BACKUP DRIVE

1 4 mm Dat Tape Drive
X EXIT DAILY BACKUP

OPTION:

Enter 1 for tape drive or X to Exit.

If your daily back-up needs more than one tape, it will display "end of media type device file name" on your terminal. The SA should type the device file name of the drive selected at the beginning of this run. For cartridge tape drive type /dev/rmt/c0s0.

- Weekly Back-ups. Weekly system back-ups should be accomplished by the SA to capture the following file systems: /osexec, /informix, and /work. The weekly back-up should be run on the same day of each week to assure all data is captured. To run weekly back-ups, perform the following tasks:

  - Ensure that no user is on the system.
  - Login as root.
  - Open a Terminal Window.
  - Type ./osexec/sysbkp or cd /osexec; ./weekly
  - Enter "w" for weekly back-ups.
  - Enter the number for the appropriate tape drive.

- Monthly Back-ups. A monthly system back-up should be performed by the SA to capture an image of the "root" (/) file system. The monthly back-up should be performed near the end of the month and on the same day of each month. This can be done during the EOD process. However, you must ensure that no user is logged on the system, and that you login as "root". It is recommended the monthly back-up is not run on the same day as EOD/EOM.

  To run the monthly back-ups, perform the following tasks:

  - Ensure that no user is on the system.
  - Login as root.
  - Open a Terminal Window.
  - Type /osexec/sysbkp or cd /osexec; ./monthly.
  - Enter "m" for monthly back-ups.
  - Enter the number for the appropriate tape drive.

- Database Back-ups. AFMIS application software provides several types of back-ups. The UNIX shell script 'budbc' will back-up the TISA database tables and place them in "/informix/backup". This script should be executed on a daily basis prior to running EOD. This means that all tables affected during the day, plus tables unaffected during the day will be backed-up. You should ensure that no user is logged on the system. Usually, this script is run once a day, but can be run more than once a day. The budbc script may be executed. You may use budbc before CAO

does anything to the database as this provides a source to restore your database. To run budbc, perform the following tasks:

- Ensure that no user is logged on the system.
- Login as afmis.
- Open a Terminal Window.
- cd /work/acct/afmis/bin/util
- Type budbc a. The "a" represents the first run for that day. If the SA has to make another budbc run, to type budbc b. The back-up of the tables needs the following format:

  [table name]P[julian day]a.z, for example, mifP018a.z

mif	-	table name
P	-	production
018	-	julian day, 18th day of the year
a	-	first run for that day
.z	-	pack the file.

  See Figure 7.1-1 for the data layout in the file.

```
8920007535776|BREAD WHITE|LB|0.4272|19.444|E|0.4272|10/01/1993|19.444|0.0|
8920007535779|BREAD WHOLE WHEAT|LB|0.4272|6.263|E|0.4272|10/01/1993|6.263|0.0|
8910005846435|MILK HOMOGENIZED|GL|1.6447|2.238|E|1.6447|07/01/1993|25.0|0.0|
8910001516497|MILK LOWFAT|GL|1.5702|22.762|E|1.5702|07/01/1993|12.5|0.0|
8920007535768|ROLLS HAMBURGER|LB|0.5488|11.794|E|0.5488|10/01/1993|11.794|0.0|
```

FIGURE 7.1-1 - Layout of Data (UNLOADED Format)

- EOD/EOM Back-up. During the EOD process, the DFO and TISA databases are backed-up. The End-of-Day Part I backs-up the TISA, TISA-W, and IFA database. The back-up files are created in the '/informix/backup/tisa' directory. The DFO database is backed-up during the DFO End-of-Day process. These files are created in '/informix/backup/dfo' directory. The databases are backed-up to tape the next day by the SA by executing the following instructions:
  - Login as afmis <RETURN>
  - Type cd /work/acct/afmis/bin <RETURN>
  - Type. /ajk71u.x01<RETURN>

Note: End-of-Day menu will vary depending on whether you are a Standard dining facility user or an AHC user.

- For a standard dinning facility user, choose the options you wish:

  EOD OF DAY BACKUP

  A Backup AHC End-of-Day
  D Back-up DFO End-of-Day
  T Back-up TISA End-of-Day
  B Back-up TISA and DFO End-of-Day
  X Exit

- For an AHC dinning facility user, choose the options you wish:

  EOD OF DAY BACKUP

  A Backup AHC End-of-Day
  D Back-up DFO End-of-Day
  T Back-up TISA End-of-Day
  B Back-up AHC, TISA and DFO End-of-Day
  X Exit

  After a successful execution of ajk71u.x01 the 'informix/backup/dfo' and informix'/backup/tisa' directories are cleaned.

7.2 File Recovery

During the course of normal operations, the SA may be required to recover missing or corrupted files, directories, and/or entire file systems from the system back-ups. It is imperative the source of the problem that resulted in a lost file or damaged file system be determined before a recovery procedure is implemented. The methodology of analyzing and resolving problems will be discussed in Section ??. The SA must determine what files are to be recovered from back-up media. When the directories, file(s), or file system(s) have been identified, the SA must restore the missing items in the same manner that the back-up was created. It is imperative that you have a good back-up. The following represent some of the most frequently used recovery procedures:

- Individual Recovery. In order to recover individual files or directories from the back-up media, the SA first determines when the file was lost or damaged. The SA should retrieve the most current back-up media from the tape library that contains the file or directory and place the media in the appropriate machine device on the Unix Server. Normally, a temporary directory is created to hold the file or directory read from the tape media. After the file or directory has been loaded to the temporary directory, the SA should check to be sure that no corruption or damage exists

before the file/directory is restored to the proper address. If the SA performed the back-up using shell scripts, then the "restore" procedure will have to be executed using a similar command from the command line. It is the responsibility of the SA to double-check all files and directories to verify that system integrity has not been compromised during execution of the recovery procedure. The following command can be used to recover a single file (**ensure you are in the root directory**):

cpio -icvBdum [‘path to file’] < /dev/rmt/c0s0
i.e. cpio –icvBdum ‘work/acct/afmis/user.txt’ < /dev/rmt/c0s0

- File System Recovery. The recovery procedures used to restore individual files or directories may also be used to recover entire file systems if corruption or damage is detected during normal system operations. The SA should be aware that file systems often require large amounts of system space. Careful consideration should go into planning when and how a file system will be restored, before a specific recovery procedure is executed. The SA should make sure, before and after the file system has been restored, that no corruption exists that could hinder system performance and integrity.

  To restore a file system, it must be determined that it is corrupted. Follow these steps to restore all the files in a file system (**ensure you are in the root directory)**:

  - Login as root.
  - Mount the latest tape with the file system, for example, weekly has /osexec, /work, and /informix
  - cpio -icvBdum [file system] < /dev/rmt/c0s0
  - Total System Recovery. If a catastrophic system event causes a crucial hardware or operating system malfunction, the SA may be required to recover the entire system or large parts of the system from back-up media. After repairing the malfunction, the SA should follow the procedures for reloading the OS, see Appendix B. At this point, the SA should determine what needs to be restored, and follow procedures from the Individual or File System Recovery Sections of this manual. The SA is responsible that the most current versions of the back-ups are used, and verifying the files or file systems are not damaged or corrupted, before and after restoration has been executed.

- System Crash Recovery. When a system stops operating due to a power fluctuation, lack of minimal working space, or other random problems, the effect is in essence a "crash." A "crash" is simply the abrupt and total loss of operations for a brief period of time and usually requires simple recovery procedures to resume processing. The SA should be aware that if a system crashes on a regular basis, there may be a larger problem that could cause permanent loss of hardware and/or software. To recover from a system crash, the first step is to bring the system back to

single- user mode and check the system disks with appropriate command(s). If the crash was severe and the system disk was damaged beyond repair, the SA must call COMPAQ.

7.3 Restoring the TISA/IFA database from back-up

Restoring the database files that were backed-up by ajk71u.x01. If the End-of-Day/End-of-Month function encounters a fatal error during execution, the CAO should be contacted. If necessary, the system administrator may have to restore the database(s) from back-up.

1. Log on the system as "afmis".

2. If back-up is on tape, place contents of tape onto disk using utility program ajk72u.x01 located in $HOME/bin. If back-up is currently on disk in directory $EODBKUP/tisa, skip to STEP 3.

   a. Key enter: cd $HOME/bin/tape <RETURN>

   b. Key enter: ajk72u.x01 <RETURN>

   c. Select option "T" (TISA) from menu displayed. Press <RETURN>

   d. Follow program directions.

   If an error occurs while attempting to place the contents of the tape on disk, contact system support. DO NOT CONTINUE.

3. Key enter: cd /inforrmix/tisa/afmis.dbs <RETURN>

4. Key enter: ls -C <RETURN>

5. Make sure that you are in the directory containing the TISA/IFA database.

6. Key enter: rm * <RETURN>

7. Key enter: cd $EODBKUP/informix/tisa <RETURN>

8. Key enter: ls | cpio -pm /tisa/afmis.dbs <RETURN>

   If an error occurs while copying the database, contact CAO. DO NOT CONTINUE.

9. Key enter: cd /informix/tisa/afmis.dbs <RETURN>

10. Key enter: chgrp informix * <RETURN>

11. Key enter: cp /dev/null $TRLOG/trlog <RETURN>

12. Key enter: ls -1 $TRLOG/trlog <RETURN>

13. Make sure the trlog has no contents (size=0).

14. Key enter: cd $HOME/bin/dbadmin/sql <RETURN>

15. Create the following SQL using "vi" if it does not currently exist:

    {maxrpt.sql}

    SELECT MAX(rpt_num) from rel

16. Key enter: isql afmis maxrpt <RETURN>

17. Record report number retrieved by the SQL on a piece of paper.

18. Key enter: cd $AFMIS/reports <RETURN>

19. Remove all reports with numbers greater than the maximum report number recorded. (Report naming convention is R########## or R######## .Z where "##########" is a number.)

20. Key enter: ls -lt | pg <RETURN>

21. The report number displayed at the top of the list should match the maximum report number recorded. If not, repeat steps 19 through 21.

22. Key enter: cd $HOME/bin/dbadmin/sql <RETURN>

23. Key enter: isql afmis CHKTABLE >> chk.out <RETURN>

24. Ensure there are no database errors. Repair any errors found. NOTE: You may want to use 'grep -i error chk.out' to detect errors.

7.4 Restoring the DFO database from back-up

1. Log on the system as "afmis".

2. Open a Terminal Window.

2. If back-up is on tape, place contents of tape on disk using utility program ajk72u.x01 located in $HOME/bin. If back-up is currently on disk in directory $EODBKUP/dfo, skip to STEP 3.

   a. Key enter: cd $HOME/bin/tape <RETURN>

   b. Key enter: ajk72u.x01 <RETURN>

   c. Select option "D" (DFO) from menu displayed. Press <RETURN>

   d. Follow program directions.

   If an error occurs while attempting to place the contents of the tape on disk, contact system support. DO NOT CONTINUE.

3. Key enter: chmod 777 $EODBKUP/dfo/* <RETURN>

4. Sign off the system.

5. Sign on as "dfosa".

6. Key enter: cd /informix/dfo/afmis/afmisdb.dbs <RETURN>

7. Key enter: ls -C <RETURN>

8. Make sure that you are in the directory containing the DFO database.

9. Key enter: rm * <RETURN>

10. Key enter: cd $EODBKUP/dfo <RETURN>

11. Key enter: ls | cpio -pm /informix/dfo/afmis/afmisdb.dbs <RETURN>

If an error occurs while copying the database, contact system support. DO NOT CONTINUE.

12. Key enter: cd /informix/dfo/afmis/afmisdb.dbs <RETURN>

13. Key enter: chgrp informix * <RETURN>

14. Key enter: cd /informix/trlog/dfo <RETURN>

15. Key enter: cp /dev/null trans.log <RETURN>

16. Key enter: ls -l trans.log <RETURN>

17. Make sure that the trans.log has no contents (size=0).

18. Check all database tables for corruption. Repair any errors found.

7.5 Restoring TISA Database Files/Tables from Hard Disk

The TISA/IFA database files/tables are backed-up by budbc script and End-of-Day Part I. Budbc places the back-ups on disk in /informix/backup, as an unloaded flat file (Figure 7.1-1). To restore from the budbc back up, the file/table, in question, must be dropped from the database. Next, the file/table must be created and the data loaded from /informix/backup/[table name]. Finally, the indexes of the file/table must be created. The procedure for each of the steps is located in the INFORMIX/SQL Section 5.

Caution must be used when restoring specific tables. Some tables contain data directly related to data on other tables. It may be dangerous to restore a single table without restoring other tables that have data links. CAO should be consulted before attempting this process.